# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*

| | | |
|---|---|---|
| 1. REPORT DATE<br>**2010** | 2. REPORT TYPE | 3. DATES COVERED<br>**00-00-2010 to 00-00-2010** |

| | |
|---|---|
| 4. TITLE AND SUBTITLE<br>**Air Force Cyber Command (Provisional) Decision Support** | 5a. CONTRACT NUMBER<br>5b. GRANT NUMBER<br>5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER<br>5e. TASK NUMBER<br>5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**Rand Corporation,1776 Main Street,PO Box 2138,Santa Monica,CA,90407-2138** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S)<br>11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT<br>**unclassified** | b. ABSTRACT<br>**unclassified** | c. THIS PAGE<br>**unclassified** | **Same as Report (SAR)** | **37** | |

# Air Force Cyber Command (Provisional) Decision Support

Richard Mesic, Myron Hura, Martin C. Libicki,
Anthony M. Packard, Lynn M. Scott

Prepared for the United States Air Force

Approved for public release; distribution unlimited

RAND PROJECT AIR FORCE

The research described in this report was sponsored by the United States Air Force under Contract FA7014-06-C-0001. Further information may be obtained from the Strategic Planning Division, Directorate of Plans, Hq USAF.

**Library of Congress Cataloging-in-Publication Data**

Air Force Cyber Command (provisional) decision support / Richard Mesic ...[et al.].
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4888-2 (pbk. : alk. paper)
1. United States. Air Force--Security measures. 2. Information warfare--United States. 3. Cyberspace--Security measures--United States. 4.United States. Air Force Space Command--Organization. 5. United States. Air Force--Operational readiness. 6. United States. Air Force--Decision making.7. United States. Air Force--Weapons systems. 8. Electronics in militaryengineering--United States. 9. Command and control systems--United States. I. Mesic, Rich

UG633.A6926 2010
358.4'1683--dc22

2010005142

Published 2010 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

# Preface

The Project AIR FORCE monograph from which this brief summary was generated sought to present a concise and accessible perspective on the issues and options entailed in realizing the Air Force leadership's vision on flying and fighting in cyberspace. The study was conducted to help clarify and focus attention on what can be done in that domain. In this way actionable initiatives could be developed that would move the Air Force forward toward the transformation implied by this bold extension of the Air Force's mission statement.

As this work was being completed in August 2008, the new chief of staff put the previously scheduled October 1, 2008, stand-up of Air Force Cyber Command (Provisional) (AFCYBER[P]) as a major command on hold so that he could consider significant decisions that needed to be made regarding the Air Force's role in cyberspace and the nature of a new command. After our research was completed, the Air Force took additional actions in February 2009 to designate 24th Air Force as the cyber numbered air force under Air Force Space Command. While some of the management and organizational issues we addressed in our study have now been overtaken by events, we believe that there remain a number of organizational and functional issues still to be resolved, and that this report can be used as a framework to (1) help the Air Force conduct a review of actions taken to date and, if appropriate, (2) implement course corrections.

The research described in this monograph is part of a RAND Project AIR FORCE (PAF) study, "Defining and Implementing Cyber Command and Cyber Warfare," sponsored by Lt Gen Robert J. Elder, Jr., Commander, 8th Air Force. The study was conducted in PAF's Force Modernization and Employment Program.

**RAND Project AIR FORCE**

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the U.S. Air Force's federally funded research and development center for studies and analyses. PAF provides the Air Force with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future aerospace forces. Research is performed in four programs: Force Modernization and Employment; Manpower, Personnel, and Training; Resource Management; and Strategy and Doctrine.

Additional information about PAF is available on our Web site:
http://www.rand.org/paf/

# Contents

# Acknowledgments

The authors very much appreciate the support of our two principal study sponsors, Lt Gen Robert J. Elder, Jr., Commander, 8th Air Force, and Joint Functional Component Commander for Global Strike, U.S. Strategic Command, and Maj Gen William T. Lord, Commander, AFCYBER(P). They opened their organizations to us and provided us access to their senior staffs when all were under intense pressure to shape and develop a new major command. They engaged with us personally in a number of stimulating discussions on these challenging topics. At the staff level, we appreciate the early support of Lt Col David Fahrenkrug, Chief of Strategy, and his replacement, Lt Col Jim Noetzel, as well as the continuing dialogue with Col Mark Ware, 8th Air Force Operations; Col Ward Heinke, Director, Air Force Network Operations Center; Lt Col Michael Convertino, Director of Staff; Col Warren Ward, AFCYBER(P) Plans and Programs; Col Stephen Luxion, Director, 8th Air Force Air Operations Center; and Maj Timothy "Chewy" Franz, AFCYBER(P), Force Development.[1]

Several other Air Force officers across commands within and related to AFCYBER(P) were also quite helpful. These included Lt Col Ramsdan, Air Force Operations, Plans and Requirements; Col Joseph Pridotkas, Commander, 67th Network Warfare Wing; Lt Col Timothy Haugh, Commander 315th Network Warfare Squadron; Michael Kretzer, Air Force Information Operations Center; Col Keith Gentile,

[1] The ranks, positions, and organizations we mention in these acknowledgments were accurate as of when we drafted this monograph. Organizational specifics have changed since, as detailed in amendments discussed elsewhere in this document.

Vice Commander, 9th Reconnaisance Wing, Beale Air Force Base; and Col Jim Jennings, Air Education and Training Command.

Given the importance of intelligence to all cyber activities, we were especially grateful for the opportunities we had to interact with Brig Gen Mark Schissler, Director of Cyber Operations, A30-C, Lt Gen David Deptula, Intelligence, Surveillance and Reconnaissance, and with Maj Gen Craig Koziol, Commander, Air Force Intelligence, Surveillance, and Reconnaissance Agency and his staff, including Col Robert Culhane and Col Jon Kimminau. Their insights on the synergy (and occasional tensions) with intelligence and operations in the cyber realms were most helpful. We also were briefed on Joint Electronic Warfare and Capabilities Based Assessments by Col Marc Magram, Director, Joint Electronic Warfare Center.

We are also extremely indebted to Brig Gen Steven Filo, who introduced us to the cyber activities at the National Security Agency (NSA), and to Maj Gen Randal Fullhart, Deputy Chief, Central Security Service, who shared his insights with us and provided us access to the appropriate people and programs at NSA. The Air Force Cryptologic Office Director, Keith Thomas, shared his organization's viewpoints and gave us a wide-ranging programmatic overview, while Lt Col Michelle Bowes gave us an assessment of program implementation status, and the 8th Air Force liaison officers to NSA, Col Morris and Col Layne, were helpful in setting up joint AFCYBER(P) and NSA interactions.

We also had the benefit of excellent briefings from the Defense Information Systems Agency's RADM Elizabeth Hight and Brig Gen Jennifer Napper, and from the Air Force Scientific Advisory Board's Thomas Saunders and Heidi Shyu. Don Hoening, Director, Air Force Programs, AT&T Government Solutions, and his staff were also very generous in sharing their time and insights on industry "best practices" with us.

Additionally, we had the benefit of gaining the U.S. Strategic Command's perspectives as a combatant command through discussions with personnel at Joint Task Force–Global Network Operations, Joint Functional Component Command–Network Warfare (Lt Col Robert Butts, in particular), and Joint Information Operations Warfare

Center. We also got a geographic command's perspective through discussions hosted by Lt Col L. C. Curry at Pacific Command; Maj David Yashimoto at Pacific Air Forces, LCDR Christopher Adams at Pacific Fleet, and Catherine Kraslawsky at NSA Central Security Service Pacific.

Several RAND staff and military fellows also provided useful insights and advice. These include Natalie Crawford, Robert Anderson, Timothy Bonds, Anne Konnath, Gary Landers, Gary Massey, Gary McLeod, Greg Rattray, Lara Schmidt, and Kelli Seybolt.

Finally, we are indebted to our formal reviewers, Alexander Levis of George Mason University, and Isaac Porche of RAND.

Karin Suede and Jane Siegel provided administrative and documentation support.

# Abbreviations

| | |
|---|---|
| AF | Air Force |
| AFCYBER | Air Force Cyber Command |
| AFCYBER(P) | Air Force Cyber Command (Provisional) |
| AFISRA | Air Force Intelligence, Surveillance, and Reconnaissance Agency |
| AFSPC | Air Force Space Command |
| AOC | air operations center |
| CNA | computer network attack |
| CND | computer network defense |
| CNE | computer network exploitation |
| CNO | computer network operations |
| COCOM | combatant command |
| DoD | Department of Defense |
| EW | electronic warfare |
| EWW | electronic warfare wing |
| I-NOSC | Integrated Network Operations and Security Center |
| IO | information operations |

| | |
|---|---|
| IP | Internet protocol |
| JFCC-NW | Joint Functional Component Command–Network Warfare |
| JTF-GNO | Joint Task Force–Global Network Operations |
| MAJCOM | major command |
| MEII | minimum essential information infrastructure |
| NAF | numbered air force |
| NSA | National Security Agency |
| PAD | program action directive |
| PAF | Project AIR FORCE |
| USSTRATCOM | U.S. Strategic Command |

# Air Force Cyber Command (Provisional) Decision Support

There is serious concern within the government and private sector that increasing dependence on networked systems designed for a friendly environment,[1] such as the Internet, may be creating dangerous vulnerabilities that malevolent actors—states, terrorists, or criminals—can increasingly exploit to harm us. Similar concerns are being raised over the vulnerabilities of Department of Defense (DoD) airborne and space networks that support military forces. Gen James Cartwright, U.S. Marine Corps, and former Commander, U.S. Strategic Command (USSTRATCOM) has said that

> America is under widespread attack in cyberspace. Unlike in the air, land, and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battlespace.[2]

To address these national and Air Force–specific concerns, the Air Force initiated a process of standing up a new cyber command. Air Force Cyber Command (Provisional) (AFCYBER[P]) was intended to

> [r]edefine Airpower … extend our global reach and power into cyberspace … Primary Mission is Warfighting: Integrate AF's

[1] Although packet switching, the Internet's primary communications protocol, *was* designed to withstand the effects of nuclear war.

[2] See Air Force Doctrine Document 2-X, *Cyberspace Operations*, draft, Washington, D.C.: Headquarters, U.S. Air Force, January 29, 2008.

> global kinetic and nonkinetic strike capability . . . through the full range of military operations.[3]

Significant decisions need to be made about this new command.[4] The RAND study team worked directly with 8th Air Force and AFCYBER(P) to help define the functions of this new command, including its interactions with other parts of the Air Force, other services and combatant commands (COCOMs), and other government agencies. The study focused on offensive and defensive computer network operations (CNO) and electronic warfare. It took the need to support kinetic and space operations into account but kept focused on network operations as the core of the accepted DoD definition of cyberspace. The goal was to provide a clear taxonomy in a strategies-to-tasks framework to facilitate a clear and convergent dialogue supporting the AFCYBER development process.

## Understanding the Mission

With decades of shared experience, as well as the visibility and dominance of Air Force air and space systems, airmen understand what it means to "fly and fight in the air." They have also come to understand that the Air Force also "flies and fights" in space. Then the Air Force added, "fly and fight in . . . Cyberspace" to its mission statement.[5] Unfortunately, this new cyber domain has proven to be harder to understand and adjust to. The current overly broad and abstract definitions of *cyberspace* cause confusion and divisiveness, both within and beyond the Air Force. There have been several definitions of cyberspace. The

[3] Robert Elder, "Air Force Cyberspace Command: Defense Technology Forum," briefing, 8th Air Force, June 14, 2007.

[4] However, as this monograph was being completed, in August 2008, a decision was made to reconsider the Air Force's roles and missions in cyberspace and the nature of any associated reorganizations.

[5] In December 2005, the Air Force changed its mission statement to: "The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests to fly and fight in Air, Space and Cyberspace."

Air Force's initial view was that it was a real (not virtual) domain covering the radio frequency spectrum and systems using it "from DC [direct current] to light."[6] A later Air Force definition is more succinct:

> Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum ... to store, modify, and exchange data via networked systems and associated physical infrastructures.[7]

On May 12, 2008, then–Deputy Defense Secretary Gordon England defined cyberspace as

> a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[8]

The language Air Force public affairs or recruiting offices use to promote the Air Force's cyber mission, as illustrated by 2008's television, newspaper, and magazine "above all" recruiting ads, has yet to reflect the analytic convergence the definitions above imply.[9] The tensions resulting from the disparity between the Air Force's publicly perceived role in and its actual more-modest investment in cyberspace may also have fueled interagency disagreements over roles, missions, and authorities—such as the national cybersecurity initiative calls

[6] Lani Kass, "A Warfighting Domain," briefing, Air Force Cyberspace Task Force, Washington, D.C.: Headquarters U.S. Air Force, September 29, 2006.

[7] Program Action Directive (PAD) 07-08, *Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER)*, Change 1, Washington, D.C.: Office of the Secretary of the Air Force, January 24, 2008, not available to the general public.

[8] Gordon England, "The Definition of Cyberspace," memorandum, Washington, D.C., May 12, 2008, not available to the general public.

[9] See, for example, the full page ad in *USA Today*, March 3, 2008, and "Air Force Ads' Intent Questioned," *Los Angeles Times*, March 30, 2008. The campaign was cancelled in the summer of 2008.

for.[10] Carefully and clearly laying out the Air Force's future role in this domain can help preempt such difficulties.

Fundamental precursor questions need clear and convincing answers. What is cyberspace, and what is the Air Force's role in the domain? What does to "fly and fight in cyberspace" mean? What, specifically, does the Air Force plan to do in cyberspace—what effects does it want to achieve? How will it achieve them? How will it know if it has achieved them? Is "cyber supremacy" a meaningful concept? Is deterrence a tractable approach to security in cyberspace? The Air Force needs a simple, direct, explicit, and actionable discussion on what AFCYBER is really about. We believe that AFCYBER can be a responsible, capable partner in a substantially wider national security effort.

A compelling case can also be made for a central cyber-focused entity to (1) "organize, train, and equip" future cyberwarriors; (2) integrate and deconflict the various cyber efforts across the Air Force; (3) manage external coordination; and (4) advocate for cyber in the Air Force corporate process. Whether this organization should be a new major command (MAJCOM), however, is less clear, particularly in today's national security environment. But creating AFCYBER cannot be just an organizational or bureaucratic exercise. Its creation should be a key element in the process of defining how the Air Force extends its operations in the new domain—how it integrates cyberoperations with operations in air and space. This journey ought to be guided by an understandable, actionable, affordable, and accepted vision.

During the course of our research, which focused on the initial plans for a cyber MAJCOM, AFCYBER, the Air Force placed them on temporary hold to assess its role in cyberspace and the responsibilities of a new command more thoroughly. The Air Force then took further steps after our research was complete:

[10] George W. Bush, "Cyber Security and Monitoring," Washington, D.C.: The White House, National Security Presidential Directive 54 (also Homeland Security Presidential Directive 23), January 8, 2008.

- The definition of *cyberspace* was refined: a physical domain including multiple interconnected computer and telecommunications networks, network operations, processors, and controllers.
- The 24th Air Force was activated as the cyber numbered air force (NAF) within Air Force Space Command (AFSPC) and designated a strategic command under a major general. It consists of an operational center and three subordinate wings: 67th Network Wing; 688th Information Operations Wing; and 689th Combat Communication Wing. It does not, however, have a separate electronic warfare wing (EWW).
- The missions for the new cyber NAF (establish, operate, defend, exploit, attack) were defined and refined to fit USSTRATCOM Unified Command Plan 2008 mission needs more precisely. These needs include supporting direct global information grid operations and defense; planning against designated cyberspace threats; planning and executing operational preparation of the environment in coordination with the Global Command and Control System; executing cyberspace operations as directed; coordinating, advocating, integrating various cyber activities; and planning, coordinating, and executing nonkinetic global strike.[11]

Recognizing that a number of organizational and functional issues are still unresolved, this monograph can be used as a framework to (1) help the Air Force review actions taken to date and, if appropriate, (2) implement course corrections. We note in footnotes how changes implemented after the study relate to observations and recommendations we made in our completed research. Where "AFCYBER" is used below, the current realization is AFSPC/24th Air Force.

[11] PAD 07-08, *Phase I of the Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command Forces*, Change 3, Washington, D.C.: Headquarters U.S. Air Force, February 20, 2009.

## Observations

Even though the ostensible rationale for establishing AFCYBER is straightforward—"cyberspace" is a new domain with emerging operations that affect core Air Force missions and capabilities—exactly what AFCYBER is to do is anything but straightforward. An explication of more concrete missions, tasks, and capabilities is necessary.

Our initial approach to elucidating more-concrete missions, tasks, and capabilities was to examine the Air Force's cyberspace strategy and doctrine and to attempt to drill down in a strategies-to-tasks analysis. This analysis was, however, handicapped by the lack of consensus on just what the boundaries of the cyberspace mission were and by the difficulty of turning these ideas about cyberspace and cyberpower into strategies and actions. The next-best course was to attempt to make the potential breadth and complexity of these issues more concrete by developing example scenarios—missions and tasks—based on our understanding of cyberspace, the roles of current Air Force commands, and the historical roles of the Air Force vis-à-vis other services and agencies in cyberspace.

These analyses certainly have not answered (or probably even asked) all the right questions, but we believe the issues we have raised can help inform the ongoing conversations on the national security implications of cyberspace and the apportionment of roles, responsibilities, and authorities to address these implications.

Taking the new DoD definition of cyberspace (which is more constrained than the Air Force's initial concept) as a starting point,[12] there are still unanswered questions:

- What does cyberspace encompass—what are its functional, organizational and legal boundaries, in general, and how does the Air Force characterize and view its cyber domain and its relationships with non–Air Force cyberspace stakeholders, in particular? What must the Air Force do to actualize its vision?

[12] England, 2008.

- National strategy emphasizes why the nation needs to secure cyberspace but how to do so is still contentious. The National Cyber Security Initiative is a responsibility of the Department of Homeland Security, which recognizes the need for strong National Security Agency (NSA) support. Other interagency players, however, are still trying to sort out and deconflict their roles, responsibilities, and authorities. The relative emphasis on mission areas and roles and responsibilities for conduct of computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE) operations are not clear. We believe that most key players across the interagency organizations have something to gain from closer cooperation and integration—in fact, that greater cooperation is a cyber *sine qua non*—but under what terms and conditions?
- From the Air Force's perspective, what are the cyber goals, objectives, and strategies reflecting its service-specific requirements, and what capabilities might it provide the COCOMs (and the nation) to meet their requirements?
- What organizations are in charge of national security cyberspace operations? USSTRATCOM (via the Joint Functional Component Command–Network Warfare [JFCC-NW] and the Joint Task Force–Global Network Operations [JTF-GNO]) would seem to be responsible for "global" DoD cyber missions, but the Air Force also has to present cyberforces to regional COCOMs.
- How much can the Air Force do on its own? How can it work with other organizations (especially NSA) to
  - assure actionable cyber situational awareness
  - conduct defensive activities without compromising effective information sharing
  - conduct offensive cyber activities whose benefits exceed their costs and risks?
- Within the Air Force, what is a cyberwarrior? Who should be responsible for organizing, training, and equipping Air Force cyberforces? What is required from *all* airmen to make them more aware of cyber threats and responses and therefore more effective

in defending not only the networks but also more able to conduct the Air Force missions dependent on the networks.

- In the end, are we headed toward strategic cyberwar, defined as state-on-state conflict carried out in cyberspace for the primary purpose of compelling the other side to accede rather than face the prospects of continued or greater pain?[13] For the most part, many of the techniques used for cyberoperations in support of military forces would be used in strategic cyberwar. Thus, the organizational implications for the Air Force in the former apply to the latter as well. That noted, strategic cyberwar raises a separate and unique set of broad issues—for example, when and how a state should respond to a cyberattack. We have chosen to address these issues in a companion volume.[14]
- **The Bottom Line:** What does it mean to "fly and fight in cyberspace"?

One problem so far in defining this new organization is that most of its roles are currently being discharged by existing Air Force organizations, programs, and activities. The electronic warfare community has a long-established berth within the Air Force. True, many of their offensive and defensive techniques resemble their cyberspace (according to the DoD definition) counterparts, but the role that electronic warfare principally plays within the overall context of Air Force operations (e.g., suppression of enemy air defenses) is quite different from what might be expected from certain cyberoperations (e.g., exerting strategic pressure on adversaries or limiting adversary freedom of action on the Internet). Cyberspace could also be a conduit for perception management actions as a subset of information operations (IO). However, in emerging constructs for cyber and IO organizations, the medium and

[13] We recognize that "warfare" in cyberspace could occur in a number of ways and could involve overt or covert actions with or without more-conventional military action at the strategic, operational, and/or tactical levels. We have highlighted this extreme concept of interstate "strategic cyberwar" as an asymptotic deterrence test case.

[14] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, Calif.: RAND Corporation, MG-877-AF, 2009.

the message are quite distinct. Finally, cyberspace, *qua* network infrastructure, is the substrate for all Air Force operations, but the work of establishing Air Force networks has long ago been assigned to its communications and computer communities. Could the work of these diverse communities profit from being folded into a single AFCYBER MAJCOM or a cyber NAF?

Organizing just the three "traditional" CNO activities into an AFCYBER MAJCOM is less problematic but still raises concerns. Start with CND. The Air Force needs to do this effectively. There is also clearly an oversight and management role to be played within the Air Force (currently discharged by the Air Force Network Operations Center and the two Integrated Network Operations and Security Centers); perhaps CND needs the kind of emphasis that only a MAJCOM could provide. There is also an opportunity, perhaps not yet fully realized, for the Air Force to leverage NSA's capabilities here. It is clear to us that, at a minimum, the Air Force must know when other DoD network defenders plan actions that could disrupt Air Force command-and-control networks. Nevertheless, most of what it takes to protect systems day to day is done in a distributed and decentralized fashion by those who administer systems—a very local function but one that must be appropriately deconflicted at higher levels. The Air Force must define its role in "active response" (which we use rather than the term "active defense," which carries some unintended negative connotations) in a manner that allows integration into national-level processes.

CNE and CNA are closely related, especially in dealing with Internet-based networks. The techniques needed for one overlap greatly with the techniques needed for the other—notably, accessing computers and leaving something behind in the target system to do one's bidding later on. CNE, however, is clearly the domain of NSA within DoD. Both NSA and the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) have Title 50 authorities, although Title 10 missions (which is to say, attack roles) can be conducted via seamless interfaces between the Title 50 and some Title 10 elements. NSA greatly outspends the Air Force in cyberspace operations; the Air Force does not and cannot spend at the same level as NSA, but it can and does leverage NSA's investments and access. The question of just how much overlap and synergy is possible between the Air Force's and NSA's cyber interests and needs is still open (e.g., the importance of NSA's operations in the Internet's transmission control protocol and Internet protocol (TCP/IP) world relative to the Air Force's interest in non–Internet protocol, noncommercial wireless networks, such as an Integrated Air Defense System and airborne networks). Additionally, NSA is *not* focused on electronic warfare or IO.

The Air Force's current CNO focus is on CND, which is understandable and appropriate given the Air Force's increasing dependence on networks. CND is more than building better firewalls and antivirus software. Consequently, CND requires tightly integrated CNE support to allow defenders to see the threats coming before they have done their damage (and perhaps to allow the Air Force to reach out into the adversary's cyber systems using CNA for "active response").

As the Air Force and others endeavor to establish increased cyber capabilities, they must account for the following realities and issues:

- Cyberspace, even in the DoD definition, is still very broad and complex. How will the Air Force construct integrate with joint and national approaches?
- Threat realities are difficult to assess, but perceptions are being shaped and politicized by actions that may or may not be indicative of the emerging challenges (e.g., events in Estonia and Georgia[15]). What role could the Air Force play in such cyber conflicts, if any?
- DoD will have to cope with reduced fiscal resources and limited programming flexibility as it rebuilds and recovers from the post–Cold War stresses on the military. The Air Force must focus on the funding and manning of its cyber capability. What investments will make the most tangible contribution to establishing value-added cyber capabilities?
- There are many cyber stakeholders and players within all agencies of the national government and commercial organizations,

[15] See Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times*, May 29, 2007.

especially within the commercial organizations associated with critical infrastructures so dependent on cyber infrastructures. Air Force programs and operations are highly dependent on information and networks operated by commercial partners. What roles can the Air Force play in interacting with these stakeholders outside DoD?
- The terrain of cyberspace is heterogeneous—commercial, civil, and military; domestic, foreign, multinational, and global.
- How can the Air Force effectively demonstrate that it is part of a DoD–national team?

## Recommendations

These unresolved issues and realities suggest the need for a measured approach to resolving the future of Air Force cyber efforts, focusing initially on the most important and least contentious cyber mission: assuring robust Air Force air, space, and terrestrial network operations, that is, CND. AFCYBER(P) accepts this focus on network defense and information assurance. We further believe that the command's next objectives should be to

- improve situational awareness—not only of Air Force networks but also of upstream joint and interagency network activities and of the risks of relying on critical infrastructures shared with commercial partners
- integrate enhanced active responses into network operations (in collaboration with others)
- integrate active cyberspace defenses (and selected offensive cyber capabilities) with kinetic operations in air operations centers (AOCs).

Will establishment of the 24th Air Force within the cyber MAJCOM enhance CND capabilities by

- becoming the advocate for the development and funding of Air Force network operations capabilities?
- leveraging available internal Air Force, joint, and interagency capabilities?
- helping to refine requirements for active defense capabilities?

Air Force CND operations need to look both inside service-controlled networks and outside, into the global networks that the Air Force depends on but does not control (this is why Air Force interfaces with others is so critical).

Other questions still to be resolved center on the value of the entities involved and their organizational realignments:

- the alignment of Air Force Network Operations Center and the increased centralization of CND operations at the Integrated Network Operations and Security Centers
  - What is the right balance of CND capabilities between decentralized, local defense and more-centralized provision of situational awareness and active response capabilities?
- establishing improved external interfaces with
  - USSTRATCOM (JTF-GNO) and NAFs designated as COCOM components ?
  - AFISRA and NSA for necessary CNE support?

In light of these unresolved issues and near-term objectives, we offer the following recommendations:

1. Exploit the transition period to better manage expectations. The Air Force is building its cyberforces to assure its ability to fly and fight in a cyber threat environment.
2. Sharpen the definition of cyberoperations. Key issues, in the form of questions, with our suggested responses, are as follows:

| | |
|---|---|
| Is cyber the same as IO? | No. Cyber is only a medium for its own share of IO, e.g., directed psychological operations. |
| Do cyberoperations entail building and using networks? | Yes. "Establishing the domain" is part of the AFCYBER foundation. |
| Does cyber include electronic warfare? | Perhaps. It is true that analog and digital systems and applications are merging in synergistic applications, but whether including electronic warfare in AFCYBER helps or hurts electronic warfare deserves more study, particularly because, at present, not all electronic warfare would be integrated into AFCYBER. Further fractionation of the electronic warfare community and its capabilities does not seem likely to add value.[a] |
| Does cyber include CND? | Yes, to include active response. But cyber is much bigger than CND. |
| Is cyber about more than just networks? | Yes, it is also about the security and reliability of databases and the algorithms that are embedded in all our weapon systems, whether the AOC or F-22.[b] |

[a] Since our research was completed and in response to PAD change 3, the Air Force has removed the 450th EWW from the administrative control of the 24th Air Force, thus defining the scope of the cyber NAF responsibilities more specifically.

[b] This was a recent and serious concern for the Air Force Scientific Advisory Board but was beyond the scope of the study reported in this monograph.

3. Define the operational missions, required capabilities, and force structure across the cyber spectrum on which the Air Force plans to focus its efforts. Ultimately, AFCYBER should develop an investment strategy for network operations and defensive and offensive capabilities for cyberspace. To expedite this, it may be desirable to create a formal general officers' cyberspace forum to establish roles and missions for the Air Force in cyberspace and to develop definitive resource requirements and programming approaches.
4. Strengthen the relationship between AFCYBER and NSA, building on AFISRA's current and evolving authorities and operations. The Air Force is not in a position to match NSA in terms of money or manpower—it must support, leverage, and

help shape NSA's investments and operations. Determine where the integration potential and synergy are greatest, and make it so.

5. Focus on CND, including active responses. If anything, go overboard in saying so. Such a focus is
   a. necessary to keep the Air Force (literally) flying
   b. is nonthreatening to sister services and others and will also likely absorb the overwhelming share of Air Force cyberoperations resources and probably even the bulk of AFCYBER's resources.
6. Develop systems and procedural hedges against the most worrisome cyber vulnerabilities and threats. The overlay of a conceptual minimum essential information infrastructure (MEII) to protect critical functionalities may be one such approach.[16]
7. Determine which AFCYBER organizational structure (e.g., AFCYBER NAF embedded in an existing MAJCOM, such as Air Combat Command or AFSPC, or a new AFCYBER MAJCOM) can best help defend the Air Force's networks—air, space, and terrestrial.[17] Although most network defense needs to take place at lower levels of the organizations, some critical functions do need high-level, centralized direction and execution (e.g., standards, tools development, triage, and specialized response capabilities to counter advanced, persistent threats).
8. The extent to which the Air Force needs to develop niche CNA capabilities is more of an operational military than an intelli-

[16] The term *minimum essential information infrastructure* refers to a RAND concept modeled after the U.S.'s Cold War Minimum Essential Emergency Communication Network, designed to be a bare-bones but robust means of distributing emergency action messages to nuclear deterrent forces. As far as we know, the notional MEII concept has yet to be developed. The MEII specifications must evolve out of an understanding of context-specific mission-essential functions to provide mission assurance, but efforts to determine these are notoriously difficult. See Robert H. Anderson, Phillip M. Feldman, Scott Gerwehr, Brian K. Houghton, Richard Mesic, John Pinder, Jeff Rothenberg, and James R. Chiesa, *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, Santa Monica, Calif.: RAND Corporation, MR-993-OSD/NSA/DARPA, 1999.

[17] Since our report was completed, the Air Force has established a cyber NAF (24th Air Force) under an existing MAJCOM (AFSPC).

gence decision. The Air Force should, with discretion, develop selective offensive capabilities enabled by intelligence operations in cyberspace. The Air Force should also develop disruptive capabilities to deny adversaries use of targeted portions of the cyberspace medium. Intelligence operators know how to access and exploit networks (CNE). They may know how to disrupt and corrupt networks, but can they understand, predict, and observe (e.g., provide timely cyber damage assessments) the effects—both desired and undesired—that their actions will have on an adversary's ability (or our own) to wage war?

9. Develop an analytical foundation for
    a. assessing the benefits and risks of cyberoperations (both offensive and defensive) in an effects-based context to facilitate integration and deconfliction of cyber and kinetic operations
    b. measuring the likely return on cyber-specific investments to answer one critical question: How much is enough?
10. AFCYBER should leverage existing AFISRA-NSA relationships and activities to develop Air Force offensive cyber capabilities and integrate them with kinetic operations to support JFCC-NW and NAFs designated as COCOM components. (Is the creation of the 624th Operations Center in the proposed 24th Air Force the right way to accomplish these goals?)

## Summary

Many important issues need to be resolved. The Air Force needs to

- articulate its cyber goals and objectives more clearly
- identify strategies, missions, and tasks within its purview
- continue to develop cyberforces with capabilities to ensure Air Force–specific needs are met.

We believe there is more to military cyberoperations than those outlined for the more-limited defensive cybersecurity initiatives across the government overall. The regional and functional COCOMs have two concerns relative to cyber: (1) mission assurance (the ability to conduct operations in a degraded cyber environment, in which CND will hopefully limit the degradation) and (2) integrated attack (of which CNA is just one element). We believe that the Air Force's goal should be to posture its cyberforces for the broader context—integrated air, space, and cyberoperations in support of joint operations, with initial emphasis on integrating these *regional* operations in an AOC under the control of a joint force air component commander, while, at the same time, engaging more proactively with USSTRATCOM to help shape and conduct *global* cyber missions, day to day and in crisis and war, through the JFCC-NW and JTF-GNO.[18]

But the Air Force will have to address other key cyber issues we have discussed here through cooperative efforts with its sister services and other interagency organizations. To fully meet its vision of flying and fighting in cyberspace, the Air Force will need to proactively address the partitioning of cyber responsibilities and authorities across DoD and, eventually, perhaps, across the interagency organizations that will be responsible for defending the nation in cyberspace. Credibility built on established cyber capabilities within the Air Force's purview is a prerequisite for fulfilling this vision.

Finally, we focused on computer network system-assurance aspects of cyberspace. We recognize, however, that cyberspace is really an *information* domain, and that information has strong cognitive implications. Information assurance is the defensive goal, while the ability to exploit, disrupt, and/or deceive adversary information systems and cognition is the offensive goal. Broadening the cyberspace discussion to include these cognitive dimensions and applications adds layers of complexity, opportunity, and risk that were beyond the scope of this monograph. Nevertheless, we encourage the Air Force not to lose sight of the fact that it is these less-tangible cognitive elements that are critical and that the network hardware and software are simply the tangible enablers. Cyberstrategy and tactics, techniques, and pro-

[18] In a memorandum dated June 23, 2009, the Secretary of Defense established U.S. Cyber Command under USSTRATCOM, replacing both JTF-GNO and JFCC-NW.

cedures are only beginning to touch on the IO opportunities and risks that these technologies enable, especially in the context of irregular warfare against nonpeer asymmetric adversaries that can become near peers at exploiting information networks, such as the Internet.

# Bibliography

8th Air Force, "Concept of Cyber Warfare," Operational Concept, June 1, 2007, not available to the general public.

Air Combat Command, *Enabling Concept for Airborne Networking*, Langley AFB, Va., March 18, 2008.

"Air Force Ads' Intent Questioned," *Los Angeles Times,* March 30, 2008.

Air Force Cyber Command (Provisional), *Concept of Cyber Warfare*, November 26, 2007, not available to the general public.

———, *Air Force Cyber Command Strategic Vision*, March 2008a.

———, "Part One: Vision Statement," in *Air Force Cyber Command Strategic Vision*, March 2008b

———, Programming Plan 08-01, Air Force Cyber Command MAJCOM Activation, May 22, 2008c, not available to the general public.

Air Force Doctrine Document 2-X, *Cyberspace Operations*, draft, Washington, D.C.: Headquarters, U.S. Air Force, January 29, 2008.

Air Force Instruction 13-1AOC, Vol. 3, *Operational Procedures: Air and Space Operations Center*, Washington, D.C.: Department of the Air Force, August 1, 2005.

Air Force Network Operations Center, *Air Force Cyber Control System Concept of Operations (CONOPS)*, October 13, 2007, not available to the general public.

Anderson, Robert H., Phillip M. Feldman, Scott Gerwehr, Brian K. Houghton, Richard Mesic, John Pinder, Jeff Rothenberg, and James R. Chiesa, *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, Santa Monica, Calif.: RAND Corporation, MR-993-OSD/NSA/DARPA, 1999. As of November 12, 2009:
http://www.rand.org/pubs/monograph_reports/MR993/

Antón, Philip S., Robert H. Anderson, Richard Mesic, and Michael Scheiern, *Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology*, Santa Monica, Calif.: RAND Corporation, MR-1601-DARPA, 2004. As of October 2, 2009:
http://www.rand.org/pubs/monograph_reports/MR1601/

Brackney, Richard C. and Robert H. Anderson, *Understanding the Insider Threat: Proceedings of a March 2004 Workshop*, Santa Monica, Calif.: RAND Corporation, CF-196-ARDA, 2004. As of October 2009:
http://www.rand.org/pubs/conf_proceedings/CF196/

Bush, George W., "Cyber Security and Monitoring," Washington, D.C.: The White House, National Security Presidential Directive 54 (also Homeland Security Presidential Directive 23), January 8, 2008.

Cartwright, James E., "Joint Functional Component for Network Warfare—Implementation Directive," memorandum to the USSTRATCOM Joint Functional Component Commander for Network Warfare, Offutt AFB, Neb., SM015-05, January 20, 2005a.

———, "Joint Task Force for Global Network Operations—Implementation Directive," memorandum to the Commander, Joint Task Force for Global Network Operations, Offutt AFB, Neb., SM197-05, August 5, 2005b.

———, "Joint Information Operations Warfare Command—Implementation Directive," memorandum to the Commander, Joint Information Operations Warfare Command, Offutt AFB, Neb., July 7, 2006.

Department of the Air Force, "Fiscal Year (FY) 2009 Budget Estimate, Military Personnel Appropriation," briefing, Washington, D.C., February 2008.

Elder, Robert, "Air Force Cyberspace Command: Report to CSAF," briefing, 8th Air Force, March 23, 2007.

———, "Air Force Cyberspace Command: C2 GOSG Update," briefing, 8th Air Force, May 23, 2007.

———, "Air Force Cyberspace Command: Defense Technology Forum," briefing, 8th Air Force, June 14, 2007.

———, "Defending and Operating in a Contested Cyber Domain," Air Force Scientific Advisory Board, Winter Plenary 2008, January 15, 2008.

England, Gordon, Deputy Secretary of Defense, "The Definition of Cyberspace," memorandum, Washington, D.C., May 12, 2008, not available to the general public.

Franz, Timothy, "Cyber Career Force Development: Challenges, Approach, and Current Status," briefing, 8th Air Force, August 2, 2007.

Gantz, K. F., ed., *The United States Air Force Report on the Ballistic Missile,* Garden City, N.Y.: Doubleday and Co., Inc., 1958.

Gibson, William, *Neuromancer,* New York: Ace Books, 1994.

Heinke, Ward, "Air Force Network Operations Center (AFNOC) Transformation," briefing, Headquarters 8th Air Force, November 9, 2007.

Hura, Myron, Gary McLeod, Lara Schmidt, Manuel Cohen, Mel Eisman, and Elliot Axelband, *Space Capabilities Development: Implications of Past and Current Efforts for Future Programs*, Santa Monica, Calif.: RAND Corporation, MG-578-AF, September 2007, not available to the general public.

Joint Functional Component Command–Network Warfare (JFCC-NW), Department of Defense, "All Hands" briefing, July 28, 2006, not available to the general public.

Kass, Lani, "A Warfighting Domain," briefing, AF Cyberspace Task Force, Washington, D.C.: Headquarters U.S. Air Force, September 29, 2006.

Landler, Mark, and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times*, May 29, 2007. As of February 17, 2009: http://www.nytimes.com/2007/05/29/technology/29estonia.html

Libicki, Martin C., *Conquest in Cyberspace: National Security and Information Warfare,* New York: Cambridge University Press, 2007.

———, *Cyberdeterrence and Cyberwar*, Santa Monica, Calif.: RAND Corporation, MG-877-AF, 2009. As of October 2, 2009: http://www.rand.org/pubs/monographs/MG877/

Libicki, Martin C., David C. Gompert, David R. Frelinger, and Raymond Smith, *Byting Back: Regaining Information Superiority Against 21st-Century Insurgents—RAND Counterinsurgency Study, Volume 1*, Santa Monica, Calif.: RAND Corporation, MG-595/1-OSD, 2007.

Marion, William, 67 NWW/XP, briefing to RAND, January 25, 2007.

Mesic, Richard, Robert Anderson, Myron Hura, Philip Antón, and James Chiesa, *Project AIR FORCE Perspectives on Air Force Information Warfare: A Summary Report*, Santa Monica, Calif.: RAND Corporation, MG-129-AF, 2004, not available to the general public.

Moseley, T. Michael, *The Nation's Guardians, America's 21st Century Air Force*, white paper, December 29, 2007.

O'Connell, Edward, "Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain," Newport, R.I.: Naval War College, February 21, 1997.

PAD—*See* Program Action Directive.

Program Action Directive 07-08, *Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER)*, Change 1, Washington, D.C.: Office of the Secretary of the Air Force, January 24, 2008, not available to the general public.

———, 07-08, *Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER)*, Change 2, Washington, D.C.: Office of the Secretary of the Air Force, May 2, 2008, not available to the general public.

———, 07-08, *Phase I of the Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command Forces*, Change 3, Washington, D.C.: Office of the Secretary of the Air Force, February 20, 2009.

Raines, Rich, "Center for Cyber Research," briefing, Wright Patterson AFB, Ohio: Air Force Institute of Technology, August 16, 2007.

Schneier, Bruce, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, New York: Copernicus Books, 2003.

———, *Secrets and Lies: Digital Security in a Networked World,* Indianapolis, Ind.: Wiley Publishing, Inc., 2004.

Scott, Lynn M., Raymond E. Conley, Richard Mesic, Edward O'Connell, and Darren D. Medlin, *Human Capital Management for the USAF Cyber Force*, Santa Monica, Calif.: RAND Corporation, DB-579-AF, forthcoming.

Shaver, Russell D., and Richard Mesic, *The Role of Deterrence in Counterspace Operations,* Santa Monica, Calif.: RAND Corporation, MG-547-AF, September 2007, not available to the general public.

Spencer, Larry, "America's Edge: Global Vigilance, Reach and Power," FY-09 President's Budget Briefing, Washington, D.C.: Headquarters U.S. Air Force, February 4, 2008.

Toomey, David, "Information Operations: Innovation and Integration," briefing, Lackland AFB, Tex.: Air Force Information Operations Center, May 14, 2007.

U.S. Air Force, Air Education and Training Command, "AETC Cyberspace Training Strategy," briefing, AETC/A3T, May 22, 2008.

U.S. Air Force, Scientific Advisory Board, *Implications of Cyber Warfare,* Vol. 1: *Executive Summary and Annotated Brief*, SAB-TR-07-02, August 2007a, not available to the general public.

———, *Implications of Cyber Warfare, Volume 2: Final Report*, SAB-TR-07-02, August 2007b, not available to the general public.

———, "Implications of Cyber Warfare, SAB Summer Study Outbrief to RAND," December 7, 2007c, not available to the general public.

The White House, *The National Strategy to Secure Cyberspace*, Washington, D.C., February 2003.

Wilson, Clay, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, CRS Report for Congress, Washington, D.C.: Congressional Research Service, March 20, 2007.

Wynne, Michael W., "Flying and Fighting in Cyberspace," *Air & Space Power Journal*, Spring 2007. As of February 17, 2009:
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/spr07/wynnespr07.html

———, "Letter to Airmen," May 7, 2007. As of February 17, 2009:
http://www.af.mil/news/story.asp?id=123052273

Zahirniak, Dan, Air Force Information Warfare Center, "92 IWAS Mission Brief," undated, not available to the general public.